JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – Security Policies & Controls Review
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & Mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Access Reviews (REVIEW-A)

Security Policies & Controls Review
for InfoSec & ISO/IEC standards
(using your installed ALLOut software)

Synopsis:

Review the effectiveness of your JD Edwards Information Security framework and highlight any risk exposure and potential control gaps

"Get clarity from the specialist JD Edwards security company"

Security Policies & Controls Review for InfoSec & ISO/IEC standards

(using your installed ALLOut software)

Key Features

Deliverable: An ALLOut-certified report providing a review of the effectiveness of your current JD Edwards security and system access policies, including controls and monitoring, designed to assess the effectiveness of the existing approach and identify areas where controls may be insufficient.

Approach: The audit is conducted using **ALLOut reports and inquiries** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to satisfy external audit requirements.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - with 'take control' access to your system using Teams or Quick Assist.
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Determine current Access Control Policies

- (As in ASSESS-B)
  - Business User account access vulnerabilities
  - Business User Role access vulnerabilities
  - Privileged (IT) account access vulnerabilities
  - Risks of inadvertent errors in security maintenance

Review Access Management Controls Adoption:

- Access Controls (enforceable through ALLOut configuration):
  - User accounts disabled or deleted consistently with staff turnover
  - Password policy and change frequency
  - Security Login History (F9312) and Object Usage Tracking (F989998/9) if available
  - Security Maintenance change controls and auditing
  - Role assignment documentation and auditing
  - Role Assignment requesting/restrictions (including preventative SoD enforcement)
- Access Approval (manageable through ALLOut):
  - User Access review
  - SoD exceptions and mitigations
  - Compliance controls change management auditing (including SoD rule & mitigation changes)

Highlight Risk Exposure

- Security Model
- Role Assignment Model
- Access Approval

Assess Risk Exposure -> Review & Comply -> Verify Risk Controls

JD Edwards Security Audits

(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – Security Policies & Controls Review
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & Mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Access Reviews (REVIEW-B)

Segregation of Duties Risk Review:

Breaches & Mitigating Controls

(using your installed ALLOut software)

Synopsis:

Review your JD Edwards Segregation of Duties risk exposure and highlight any control gaps

"Get clarity from the specialist JD Edwards security company"

Segregation of Duties Risk Review: Breaches & Mitigating Controls

(using your installed ALLOut software)

Key Features

Deliverable: An ALLOut-certified report providing a review of your current Segregation of Duties exposure within your JD Edwards system, using identified rules and any documented mitigations, with relevant analysis of underlying security, designed to highlight critical areas of risk and potential control gaps.

Approach: The audit is conducted using **ALLOut reports and inquiries** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to satisfy external audit requirements.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - with 'take control' access to your system using Teams or Quick Assist.
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - Your preferred SoD Rules and supporting Critical Lists must be uploaded **beforehand** (from ALLOut **SoDMaster** or entered manually). If Rules and Lists are not pre-loaded, we will use shipped 'sample' Rules and Lists only.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Determine Current Access:

- Review current SoD rules in use and fit for purpose:
  - Verify Critical Program Lists used by Rules are not missing standard JDE programs.
  - Verify no custom programs exist, or that Lists include custom programs.
  - Apply SoD Mitigating Controls (if any).
- Run User SoD Report for active Users:
  - Run Role SoD Report to identify within-Role conflicts.

Highlight Risk Exposure:

- Rule breach assessment:
  - Privileged User (IT) profiles vs Business Users.
- Security strategy:
  - Multiple Roles & the Role Chooser.
  - Deny All vs Menu Filtering with Exit security.
  - User-level security exceptions; Publicly accessible programs; Fastpath access.
  - Action Code Deny All (default permissions are read-only or update capable).
- Use of Mitigating Controls to effectively control excessive access.

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – Security Policies & Controls Review
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & Mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Access Reviews (REVIEW-C)

User Access Review
of Functional and Data Access
(using your installed ALLOut software)

Synopsis:

Review the vulnerability of your sensitive JD Edwards business data by business process, and highlight any risk exposure and potential control gaps

"Get clarity from the specialist JD Edwards security company"

Assess Risk Exposure -> Review & Comply -> Verify Risk Controls

User Access Review of Functional and Data Access

(using your installed ALLOut software)

Key Features

Deliverable: An ALLOut-certified report providing a review of the User (and role) access that is currently permitted within your JD Edwards system and any risk exposure resulting from that access.

Approach: The audit is conducted using **ALLOut reports and inquiries** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to satisfy external audit requirements.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - with 'take control' access to your system using Teams or Quick Assist.
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - Your preferred Critical Program Lists must be uploaded **beforehand** (from ALLOut **SoDMaster** or entered manually). If Lists are not pre-loaded, we will use shipped 'sample' Lists only.
  - ALLOut for E1 Version 4.1 is advised.
  - The audit can be based on **either** program access **or** menu access **or** company (row security). Unless explicitly requested, the audit will be based on Critical Program access.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Determine Current Access:

- If reporting program or menu access, verify Critical Lists exist:
  - Verify no custom programs exist (F9860), or Lists include custom programs (Configuration).
- If reporting menu access, verify Task Views used (F9000 type 00) & Menu Filtering exists.
- If reporting company access, verify active companies (F0010).
- Run User Access report:
  - Run Role Access report – verifying Role access matches Role description.

Highlight Risk Exposure:

- Critical process access assessment:
  - Privileged User (IT) profiles vs Business Users.
  - Use of Mitigating Controls to effectively control excessive access.
  - Multiple Roles & the Role Chooser.
  - User-level security exceptions.
- If reporting program or menu access, assess Security strategy:
  - Deny All vs Menu Filtering with Exit security.
  - Fastpath access; Publicly accessible programs.
  - Action Code Deny All (default permissions are read-only or update capable).
- If reporting company data access, assess impact of Exclusive vs Inclusive (see White Paper):
  - Missing *Public security; Applying *ALL vs missing tables; Missing Data items (MCU*).